

543124

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date
5 August 2004 (05.08.2004)

PCT

(10) International Publication Number
WO 2004/066196 A1

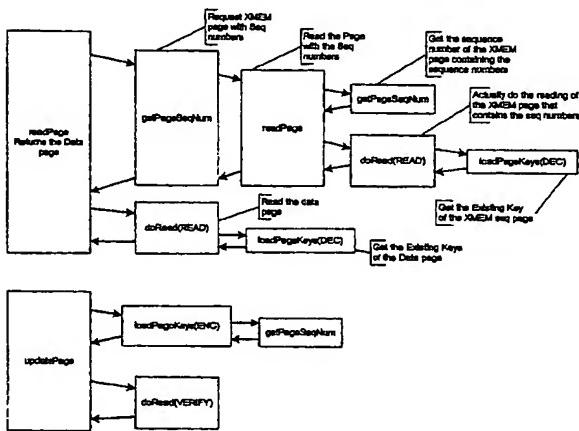
- (51) International Patent Classification⁷: **G06K 19/073**
- (21) International Application Number:
PCT/GB2004/000303
- (22) International Filing Date: 26 January 2004 (26.01.2004)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
0301726.6 24 January 2003 (24.01.2003) GB
- (71) Applicant (for all designated States except US): ECEBS LIMITED [GB/GB]; Ecebs House, 68 Dobscroft Road, Millhouses Sheffield, South Yorkshire S7 2LS (GB).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): HOCHFIELD, Barry, Sim [GB/GB]; 21 Dalserf Crescent, Giffnock, Glasgow G46 6RB (GB). BRESLIN, Anthony [GB/GB]; 21 Strathnairn Avenue, East Kilbride, Scotland G75 8FW (GB).
- (74) Agent: HARLAND, Linda, Jame; Reddie & Grose, 16 Theobalds Road, London WC1X 8PL (GB).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

[Continued on next page]

(54) Title: SMARTCARD WITH PROTECTED MEMORY ACCESS



(57) Abstract: A smartcard comprises a substrate having a smartcard chip formed on it as well as a secondary memory device, for example, a FLASH ROM, operatively connected to the smartcard chip. The secondary memory device is capable of storing a plurality of pages of data, each having associated with it a unique sequence number, the sequence number being stored separately from the data page so that when the page is to be read, the sequence number retrieved with the page can be compared with the stored sequence number to authenticate the page. To minimise the memory used on the smartcard to store the sequence numbers, some of the stored sequence numbers are stored in at least one data page stored on the secondary memory device, the sequence number for that at least one page being stored in the smartcard chip or the sequence numbers are XOR'd and the resultant digest is stored in the smartcard EEPROM. The sequence number associated with a particular page of data is incremented each time the page is modified or updated. The sequence number for each page of data is set initially at a randomly generated value, so that it is not possible to derive the sequence number from the total number of updates to the page. The smartcard of the invention thus permits the use of extended memory without compromising security.

WO 2004/066196 A1



- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.